Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
TU999029

I hereby certify that this correspondence is being transmitted by facsimile to Benjamin Lanier of the U.S. Patent and Trademark Office at 571-273-8300, on March 13, 2006.

Signature

Typed or printed name David Victor

Application Number 09/409,617	Filed October 1, 1999
First Named Inventor David M. Shackelford	
Art Unit 2132	Examiner Benjamin E. Lanier

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached 5 sheet(s).
Note: No more than five (5) pages may be provided.

I am the

□ applicant/inventor.

□ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record. 39,867
Registration number

□ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34

Signature

David W. Victor
Typed or printed name

310-556-7983
Telephone number

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

□ *Total of ______ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	D.M. Shackelford	Examiner:	Benjamin Lanier
Serial No.:	09/409,617	Group Art Unit:	2132
Filed:	October 1, 1999	Docket No.:	TUC919990029US1
TITLE:	METHOD, SYSTEM, AND PROGRAM FOR DISTRIBUTING SOFTWARE BETWEEN COMPUTER SYSTEMS		

PRE-APPEAL BRIEF REQUEST FOR REVIEW ARGUMENTS

Applicants request a pre-appeal brief review of the rejection for the following reasons.

1. Claims 1, 2, 8-14, 16, 17, 21-28, and 34-40 are Patentable Over the Cited Art

Applicants request review of the Examiner rejection of claims 1, 2, 8-14, 16, 17, 21-28, and 34-40 as anticipated (35 U.S.C. §102) by Davis (U.S. Patent No. 5,473,692) in a Final Office Action (dated December 13, 2005) and Advisory Action (dated March 2, 2006).

With respect to claims 1, 16, and 27, in the Final Office Action, the Examiner cited col. 7, lines 30-64, col. 8, lines 33-65 and col. 9, lines 15-22 of Davis as disclosing the requirements of these claims. (Final Office Action, pgs. 2-3). Applicants request review of the rejection of claims 1, 16, and 27 on the grounds that, for the following reasons, the cited art does not disclose the claim requirements of determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response and decrypting the encrypted response with the determined key if there is one determined key.

The cited col. 7 discusses how a public/private key pair may be generated and sent to a certificate system to make sure that the generated public key is unique. The cited col. 8 discusses how a first hardware agent is authenticated with a second hardware agent. The second hardware agent transmits a challenge message to the first hardware agent. The first hardware agent decrypts the challenge message with its private key and generates a response encrypting the decrypted challenge message with the public key of the second hardware agent. The second hardware agent decrypts the response wit its private key and compares the original challenge message to the decrypted response from the first hardware agent. (Davis, col. 8, lines 45-60).

Applicants request review because the cited Davis does not disclose that the authenticating node, e.g., the cited second hardware agent corresponding to the claimed first computer system, determines whether there is one key for the second computer system (corresponding to the cited first hardware agent) that can be used to decrypt the message and then decrypt the encrypted response from the claimed second computer system. In the cited Davis, the cited second hardware agent does not need to determine whether there is one maintained key for the first hardware agent to use to decrypt the message having the challenge response because the message was encrypted with the public key of the second hardware agent, not a key specific to the first hardware agent. Thus, in the cited Davis, the second hardware agent uses its own private key to decrypt the response having the challenge response, not a key for the first hardware agent that is maintained.

In other words, nowhere does the cited Davis anywhere disclose the claim requirement of determining a key for the second computer system to use to decrypt the message. Instead, the cited Davis has the second hardware agent, corresponding to the first computer system, use its own private key to decrypt the response having the challenge message, not a key maintained for first hardware agent, corresponding to the second computer system.

The claims further require that the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response. The cited Davis does not disclose this requirement because the cited second hardware agent (corresponding to the claimed first computer system) does not use the presence of a key maintained for the first hardware agent to authenticate the first hardware agent. In fact, the presence of a key for the first hardware agent is not at issue in the cited Davis for this claim requirement, because the second hardware agent uses its own private key to decrypt the message, not a key maintained for the first hardware agent as claimed. Further, according to the cited col. 8, the second hardware agent authenticates the message based on the presence of the proper challenge response, not the availability of a key maintained for the first hardware agent.

The cited col. 9 mentions that the first hardware agent initiates a request for the license token to operate the software if the second hardware agent has a valid license token. Nowhere does this cited col. 9 disclose the above discussed requirements for determining whether the second computer system is authorized to access the software based on the presence of one maintained key for the second computer system (corresponding to the first hardware agent) requesting access.

Further, the cited art does not disclose that a first computer system maintains keys of computer systems authorized to access the software, where the keys are used to determine whether a computer system is authorized to access the software. Instead, the above discussed

Davis discusses how the second hardware agent, authenticating the first, uses its own private key to decrypt the message, not a key maintained for the first hardware agent requesting access or authentication.

In the Advisory Action, the Examiner found that the above arguments are not persuasive because Davis discloses that a message is encrypted by a first node (corresponding to the claimed second computer) using the first node private key and then transmitted to a second node (corresponding to the claimed first computer) at col. 5, lines 40-56. Applicants request review of this finding for the following reasons.

The cited col. 5 mentions that a message digest is encrypted using a private key of the first node (PRK1) and that a symmetric key is encrypted with a public key of the second node PUK2), both inputted into a transmission message. The second node decrypts using its private key (SK2) and a public key (PUK1) of the trusted authority. Although the cited col. 5 discusses how a second node uses a public key to decrypt a message decrypted using a private key of the first node (PRK1), there is no disclosure in this cited section of the claim requirement that the second node (corresponding to the claimed first computer system) determine whether there is a key maintained for the second computer system to decrypt a received response, such that the second computer system (cited first node) is not allowed to access software if there is no determined key for the second computer system, i.e., first node.

In the Advisory Action, the Examiner further found that the public key of the first node PUK1 meets the limitation of determining whether there is one maintained key of the second computer system capable of decrypting the received response. Applicants request review of this finding because according to the cited col. 5 the second node does not determine whether there is one maintained key for the first node (second computer system) as claimed. Instead, according to the cited col. 5, the second node decrypts the symmetric key (SK) and the digital certificate with a published key (PUBTA) of a trusted authority to obtain the public key of the first node (PUK1). Thus, the second node does not maintain keys as claimed of systems authorized to access software as claimed, because the second node obtains the public key of the first node from a trusted authority. Moreover, there is no disclosure that the cited second node considers the presence or absence of a key for the first node to determine whether to authorize the first node to access software. Instead, the cited second node uses a published key (PUBTA) to obtain the public key, not determine whether there is a key from the first node from maintained keys of nodes or systems authorized to access the software.

For all the above reasons, Applicants request review and reversal of the rejection with respect to claims 1, 16, and 27 are patentable over the cited art, because the cited Davis does not disclose all the claim requirements.

Applicants request review of the rejection of independent claims 12 and 25 for the reasons discussed with respect to 1, 16, and 27, because the cited Davis does not disclose that the a second computer system (requesting access to the software) encrypts a response message to the first computer system, wherein the first computer may use a key provided by the second computer system to decrypt the response message to receive access to requested software in response to the encrypted response message.

Applicants further request review of the rejection of claims 9, 22, and 35 that depend from claims 8, 21, and 34 in view of the above discussed sections of Davis the Examiner cited for the additional requirements of these claims. (Final Office Action, pgs. 5-6)

The claims require that the first computer system maintain public keys from authorized computer systems and use the requesting second computer system's public key to decrypt the response with the maintained public key. The cited col. 8 of Davis mentions that the second hardware agent (corresponding to the claimed first computer system) decrypts the message from the first hardware agent (corresponding to the claimed second computer system) including the challenge response with its own private key. The cited Davis does not disclose that the second hardware agent decrypts the message including the challenge response with a public key from the second computer system. Further, nowhere does the cited Davis disclose that the second hardware agent maintain public keys from multiple authorized first hardware agents to use to decrypt their challenge response.

Applicants further request review of the rejection of claims 10, 23, and 36 that depend from claims 1, 16, and 27, where the Examiner cited col. 8, lines 33-35 of Davis as disclosing the limitation of determining whether the response includes configuration data for a system that is authorized to access the computer software. configuration data of these claims. (Final Office Action, pg. 6)

The cited col. 8 mentions that the first hardware agent, requesting authentication, outputs a message including its unique authentication device certificate to the second hardware agent.

Nowhere does this cited col. 8 anywhere disclose that the message sent by the second hardware agent (corresponding to the claimed first computer system) include a request for configuration data from the first hardware agent (corresponding to the claimed second computer system). Further, nowhere does the cited col. 8 disclose that the second computer system precesses the response to determine whether the configuration data is for a system authorized to access the computer software. Instead, the cited col. 8 mentions a unique device certificate, not a request and consideration of configuration data of the requesting system (first hardware agent) as claimed.

Applicants further require review of the Examiner's rejection of claims 5 and 31 as obvious (35 U.S.C. §103(a)) over Davis in view of Komura (U.S. Patent No. 5,994,307). (Final Office Action, pg. 10)

Claims 5 and 31 depend from claims 4 and 30, respectively, and further require that the random component included with the message is comprised of a time stamp, where determining whether the decrypted response includes the message determines whether the response includes the random component. The Examiner cited col. 7, lines 22-30 and col. 6, lines 40-67 of Komura as teaching the time stamp claim requirement. (Final Office Action, pg. 10)

The cited cols. 6 and 7 of Komura discuss how a time stamp is attached to a packet and how the time stamp is used. However, Komura concerns the use of a time stamp with a packet for communicating the packet. (Komura, col. 1, lines 5-12). Nowhere does the cited Komura teach or suggest the use of a time stamp as a random component used to determine whether a second computer system may access software. Instead, the time stamp of Komura is used for transmitting a packet without stopping event when a bit rate becomes higher. (Komura, col. 1, lines 5-12).

Dated: March 13, 2006

By:

David W. Victor
Registration No. 39,867

Please direct all correspondences to:
David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977; Fax: 310-556-7984